Press Release

United States Secret Service

Department of Homeland Security

September 15, 2020
CMR 14-20

SECRET SERVICES HOSTS CYBER INCIDENT RESPONSE SIMULATION

WASHINGTON - Today, the U.S. Secret Service hosted a virtual Cyber Incident Response Simulation with state and municipal government officials focused on ransomware attack and mitigation strategies. The training was the fourth of its kind and the second virtual event aimed at the agency's Cyber Fraud Task Force (CFTF) partners.

The training offered executives who play an active part within their organization's cyber incident response a simulated scenario to enhance planning, collaboration, and information sharing between private organizations and the Secret Service.

Event participants worked through a uniquely designed cybercrime crisis role-play simulation in order to gain a better understanding, experience, and knowledge of how to efficiently and effectively respond to a ransomware attack. Ransomware is a type of malicious software cyber actors use to deny access to systems or data. The malicious cyber actor holds systems or data hostage until the ransom is paid. After the initial infection, the ransomware attempts to spread to shared storage drives and other accessible systems. If the demands are not met, the system or encrypted data remains unavailable, or data may be deleted.

"Recognizing the dynamic nature of this threat, President Trump has made it a priority to build strong and robust cybersecurity across the federal government," said Acting Secretary Chad F. Wolf. "Developing robust partnerships with our state and local colleagues is critical to meeting that priority and accomplishing our shared goal of protecting the nation's cyber infrastructure. Your participation in this exercise is indicative of your commitment to keeping the Homeland safe from virtual threats."

As the cyber mission of the Secret Service expands, the agency has adopted a multifaceted approach inclusive of education and information sharing, and as well as the enhanced development of partnerships with industry representatives.

"Fighting cybercrime requires a 'whole of society' approach. It absolutely necessitates that all stakeholders – private and public, Federal, state, county and local – work together towards the prevention of, response to, and recovery from cyber incidents," said Secret Service Director James Murray. "Today's simulation gives us a chance to learn about each other's processes, strengths and successes, and capitalize on each other's lessons learned so that we can move more effectively when the time comes to respond."

The event featured guest speakers from across law enforcement as well as industry executives who discussed a range of topics:

- partnerships between the Secret Service, Federal Bureau of Investigation (FBI), and the Department of Homeland Security Cyber Infrastructure Security Agency (CISA);
- the complex cyber-threat environment;
- the needs of organizations victimized by cybercrime, and;
- the capabilities, investigative processes and tools of the Secret Service, specifically the capabilities of the National Computer Forensic Institute (NCFI).

To learn more about the Secret Service investigative mission, visit us at: www.secretservice.gov.